

# Information Gathering

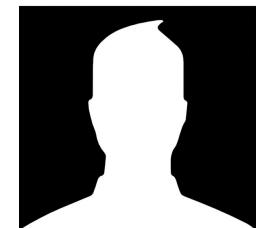
- Reconnaissance tactics and methods

Håkan Sonesson  
[hakan.sonesson@atea.se](mailto:hakan.sonesson@atea.se)  
Senior Security Consultant at Atea



# About the speaker

- **Håkan Sonesson**
  - 20 + years experience in information security field.
    - IT-security consultant (Forensics and penetration testing) at IQ AB.
    - CISO at National Courts Administration (Domstolsverket).
    - CISO at Jönköping University (JU).
    - Senior information Security Consultant at Atea (From october 2018).



# About the content in this speak

- **Only a snapshot what you can do with information gathering.**
  - Concept and mindset, not a complete overview.
    - See the last slide for more information and sources.



# About information gathering

- **Technics and methods to find information about the victim using available sources on internet.**
  - Passive and active information gathering.
    - **Passive** – More or less an attacker anonymous collecting information about the victim using publicly available information (*not from the victim's network*).
    - **Active** – Actively collecting information about the victim. For example enumerate relevant information from network services etc.



# About information Gathering

- **Important and powerful step for an attacker.**
  - The more information an attacker manage to gather about the target prior to our attack, the more likely to succeed.
  - Often victims don't understand how much information an attacker can find about an organization and/or person.
    - Small pieces of information could become sensitive together.



# About information gathering

- **Why information gathering is powerful for an attacker**
  - “*Give me six hours to chop down a tree and I will spend the first four sharpening the axe*” - (Abraham Lincoln).
  - “*If you know the enemy and know yourself, you need not fear the result of a hundred battles*” - (Sun Tzu).

## How Social Media Impacts Data Security

BUSINESS SOLUTIONS Social media is a growing security risk as a source of data leaks and misinformation. Vigilance and training are crucial to minimizing risks for individuals and business.

## Breach of Confidentiality at work

Most employees during the course of their daily working activities have access to confidential company information and/or data.

28/03/2018 15:39 BST | Updated 28/03/2018 15:39 BST

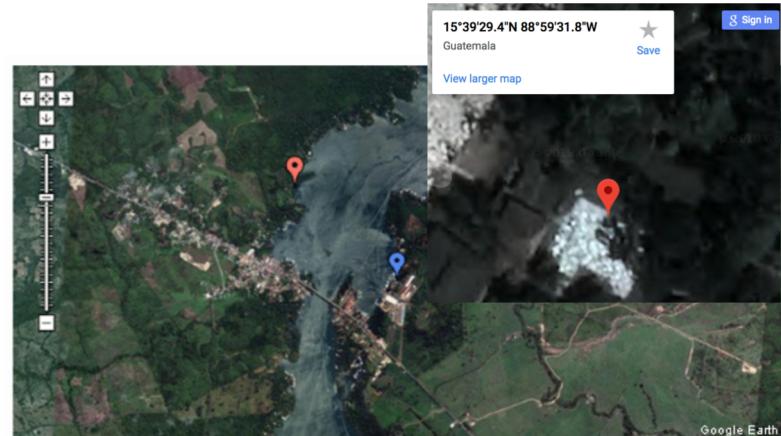
## Google Knows Literally Everything About You

# About information gathering

- Why information gathering is powerful for an attacker
  - Our footprint on the internet is vast. Even the "best" slips.

**Basic Image Information**

Camera:	Apple iPhone 4S
Lens:	4.3 mm
Exposure:	Auto exposure, Program AE, 1/20 sec, f2.4, ISO 125
Flash:	Off. Did not fire
Date:	December 3, 2012 12:26:09PM (timezone not specified) (2 hours, 41 minutes, 59 seconds ago, increasing usage because of 8 hours behind GST)
Location:	Latitude/longitude: 15° 39' 29.4" North, 88° 59' 31.8" West (-15.658167, -88.992167)
Photos on Jeffrey's blog are near this location.	
Map via embedded coordinates at Google, Yahoo, WebMaps, OpenStreetMap, Bing (also see the Google Maps pane below)	
Altitude: 7152159.665 m Terrain guess from earthworks.org: 6 hours behind GST	
File:	480 x 640 JPEG (13.41 bytes (0.11 megabytes)) Image compression: 88% 4% crop of the 3,264 x 2,448 (5.0 megapixels) original
Color Encoding:	<b>WARNING:</b> Color space tagged as sRGB, without an embedded color profile. Windows and Mac browsers and apps treat the colors randomly. Images for the web are most widely viewable when in the sRGB color space and with an embedded color profile. See my <a href="#">Introduction to Digital-Image Color Spaces</a> for more information.
Image URL:	<a href="http://avast.vicara.com/en-image/conference-mo-skag/151c4f840013c774d4d210f4fb6c75.jpg">http://avast.vicara.com/en-image/conference-mo-skag/151c4f840013c774d4d210f4fb6c75.jpg</a> Apply other tools to this image via <a href="#">imgOpn.com</a> .



**Fugitive McAfee exposed by basic geotagging feature**

# Passive information gathering

- **Explore some examples.**



# Passive information gathering

- **Scope the victims network**
  - Find IP-range with whois.

```
root@kali:/# whois -B [REDACTED].75.240
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf
%
% Information related to '[REDACTED]72.0 - [REDACTED].79.255'
```

<https://ripe.net>

# Passive information gathering

- Scope the victims network
  - Use censys.io

The screenshot shows the Censys.io web interface. At the top, there's a search bar with 'IPv4 Hosts' and a dropdown, and a status indicator '75.0/24'. On the right, there are 'Register' and 'Sign In' buttons. Below the header, there are navigation links for 'Results' (which is selected), 'Map', 'Metadata', 'Report', and 'Docs'. On the left, there's a sidebar with 'Quick Filters' for 'Autonomous System' (116), 'Protocol' (105 443/https, 75 80/http, 1 22/ssh, 1 25/smtp), and 'Tag' (105 https, 93 http, 1 smtp, 1 ssh). The main area is titled 'IPv4 Hosts' with stats: 'Page: 1/5 Results: 116 Time: 173ms Query Plan: expanded'. It lists five hosts with their IP addresses (75.146, 75.151, 75.213, 75.193, 75.64), operating systems (Windows), ports (443/https, 80/http), and specific services (Microsoft Internet Information Services 8, The page cannot be displayed, Qlik Sense login page, BIG-IP logout page). Each host entry includes a location (Copenhagen, Frederiksberg, Capital Region, Denmark) and a detailed breakdown of the gathered data.

# Passive information gathering

- Scope the victims network

- Reverse DNS with theharvester.

```
root@kali:~# theharvester -n -d [REDACTED] -b all
```

1

```
[+] Resolving hostnames IPs...

[REDACTED]: empty
Cn1.meetme.[REDACTED]: empty
Cn2.meetme.[REDACTED]: empty
Cn3.meetme.[REDACTED]: empty
Formandsator.[REDACTED]: empty
Internal.[REDACTED]: 16.57
Mailse.[REDACTED]: empty
Meetme.[REDACTED]: 75.190
aam.[REDACTED]: 118.46
aamp.[REDACTED]: 0.30
absolute-mdm.demo.[REDACTED]: 192.165.41.76
access.demo.[REDACTED]: 192.121.18.69
```

2

# Passive information gathering

- **Harvest e-mail**
  - Find e-mail addresses for login or phishing etc.

 telia.se  
Alla e-postadresser hittades för telia.se [?](#)

Mest vanliga mönstret: {first} . {last} @ telia.se 512 e-postadresser

k ■■■ stin.j.lundberg@telia.se ●	2 källor ▾
t ■■■ as.lind@telia.se ●	3 källor ▾
b ■■■ rn.a.bergstrom@telia.se ●	2 källor ▾

[Visa fler resultat](#)

# Passive information gathering

- **Googlebot (spider)**
  - More powerful than people thinks.
  - Diggs deep in organizations web services.
  - Gather words in websites and documents etc.
  - Can disclose sensitive information about the organization.



# Passive information gathering

- **Google Hacking**
  - Using Googles search operators to find specific information from an website.
    - Google Hacking Database (GHDB)



<https://www.exploit-db.com>

# Passive information gathering

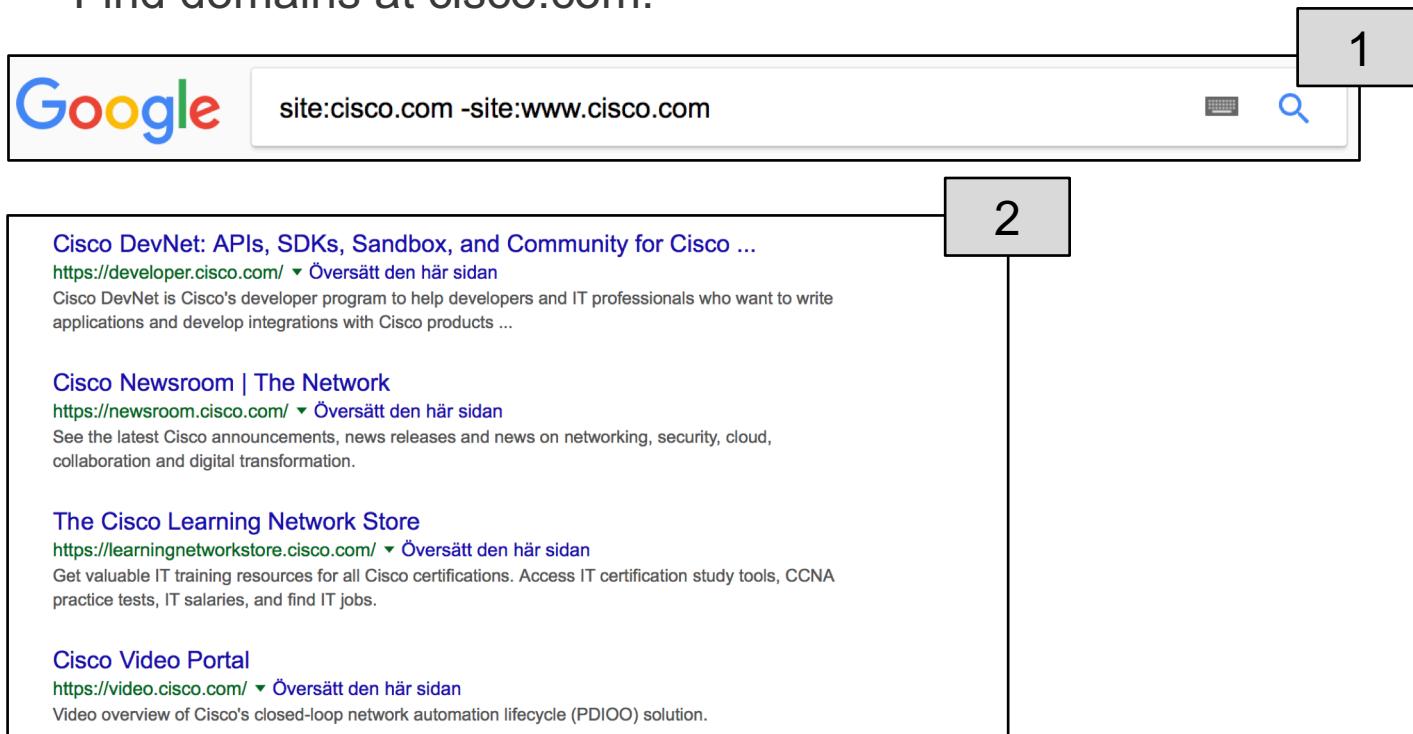
- **Google Hacking**
  - Basics
    - site:<domain.xy> (**Specific information from the domain**)
    - ext:<filetype> (**Information with specific filetype**)
    - inurl:<string> (**Websites matches the url-string**)
    - intext:<string> (**Websites matches the string**)
    - intitle:<string> (**Webtitles matches the string**)
    - cache:<domain.xy> (**View a cached copy of the website**)
    - | (**Or**)
    - || (**And**)



# Passive information gathering

- **Google Hacking**

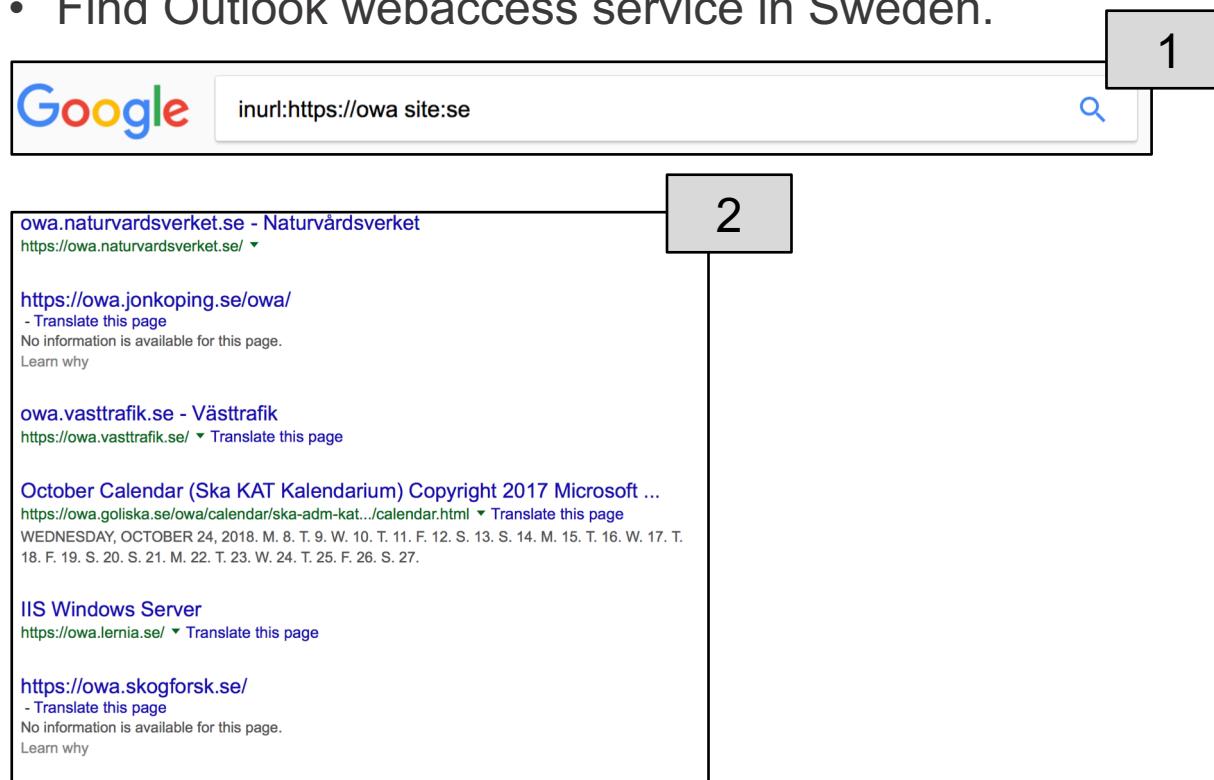
- Example
  - Find domains at cisco.com.



# Passive information gathering

- **Google Hacking**

- Example
  - Find Outlook webaccess service in Sweden.



# Passive information gathering

- **Google Hacking**

- Example

- Find web pages on Cisco that list files.

1

2

3

Index of /trex/client\_gui  
https://trex-lgn.cisco.com/trex/client\_gui/ ▾ Översätt den här sidan  
Index of /trex/client\_gui. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, ~ [ ], \_old setup.exe\_ ... 2017-03-20 11:27, 23M, [ ] ...

Index of /trex  
https://trex-lgn.cisco.com/trex/ ▾ Översätt den här sidan  
Index of /trex. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, ~ [ ], T\_Rex\_162\_VM\_Fedora\_...> 2017-03-20 11:31, 1.0G, [ ] ...

Index of /trex  
https://trex-lgn.cisco.com/trex/?C=M;O=A ▾ Översätt den här sidan  
Index of /trex. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, ~ [DIR], reports/ 2017-03-20 11:27, ~ [ ], T\_Rex\_VM\_Fedora\_21.

Index of /trex  
https://trex-lgn.cisco.com/trex/?C=S;O=A ▾ Översätt den här sidan  
Index of /trex. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, ~ [DIR], cl2017/, 2017-06-21 10:53, ~ [DIR], client\_gui ...

Name	Last modified	Size	Description
Parent Directory	-	-	-
TRex_CL2017.ova	2017-05-15 07:36	1.4G	
cl-get.py	2017-05-21 12:55	234	
cl2017.tar.gz	2017-06-21 10:53	148M	
cl2017.tar.gz.old	2017-06-21 10:51	148M	

# Passive information gathering

- **Google Hacking**

- Google Dorks, for example find sensitive information.
  - Google Hacking Database (GHDB)

Date	Title	Category
2018-10-26	inurl:phpPgAdmin intext:"Cappuccino"   intext:"Blue/Green"	Various Online Devices
2018-10-25	inurl:filebrowser.wcgp?subDir Communicate	Sensitive Directories
2018-10-24	ext:env intext:APP_ENV=   intext:APP_DEBUG=   intext:APP_KEY=	Files Containing Juicy Info
2018-10-23	inurl:/Portal/Portal.mwsl?PriNav=FileBrowser	Various Online Devices
2018-10-23	inurl:"/wp-json/" -wordpress	Sensitive Directories
2018-10-22	inurl:"/saml2?SAMLRequest="	Pages Containing Login Portals
2018-10-19	inurl:home.tcl intitle:gaia	Various Online Devices
2018-10-17	"[HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\Sessions]" ext:reg	Files Containing Juicy Info
2018-10-17	inurl:"/uddiexplorer/searchpublicregistries.jsp"	Advisories and Vulnerabilities
2018-10-17	inurl="/uddiexplorer/SetupUDDIEexplorer.jsp"	Advisories and Vulnerabilities

# Passive information gathering

- Google Hacking
  - Example

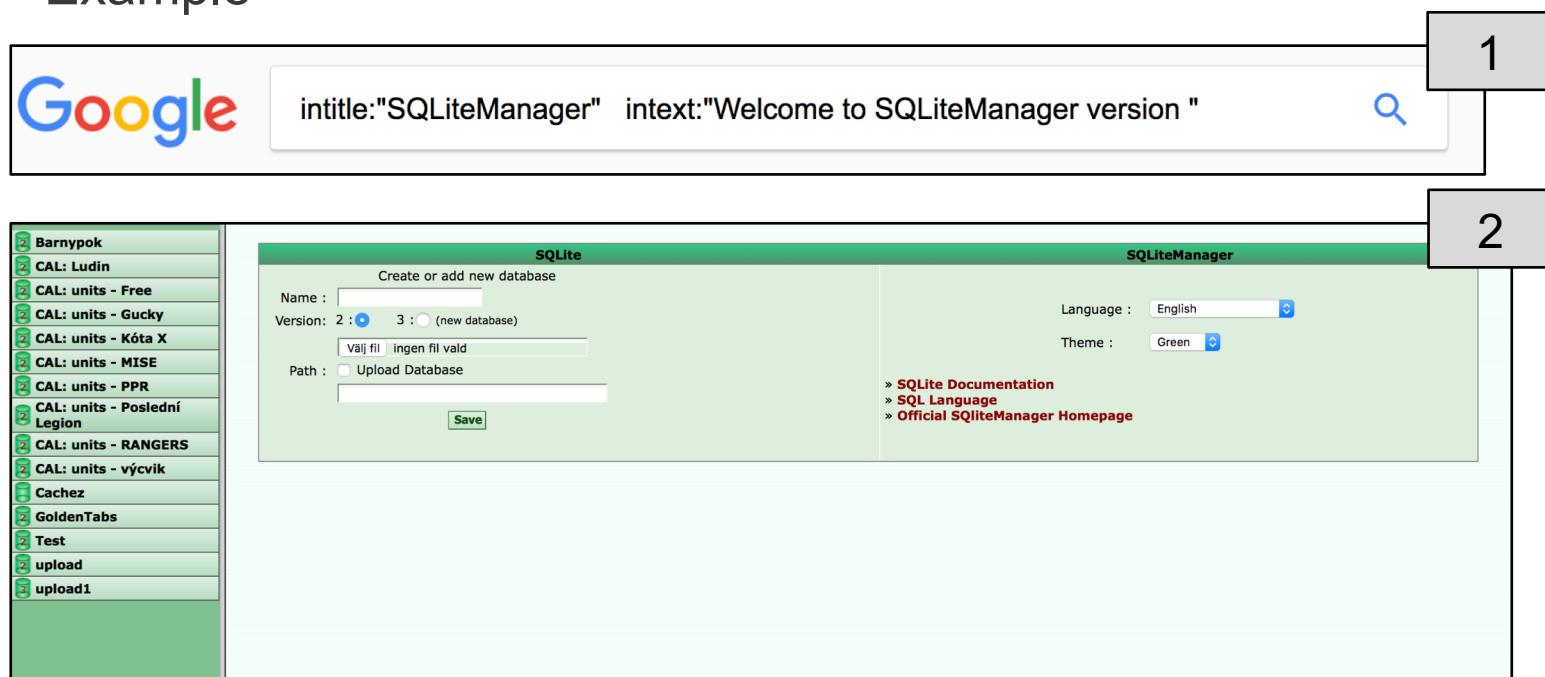
The image shows a two-panel interface. The top panel, labeled '1', displays a Google search bar with the query 'ext:env intext:APP\_ENV= | intext:APP\_DEBUG= | intext:APP\_KEY=' entered. The bottom panel, labeled '2', shows a Safari browser window displaying a list of environment variables and configuration parameters. The variables listed include:

```
APP_KEY=base64:rH21gDONKFQ4sToz1vLpbUPCWoZbSc8cv  
APP_DEBUG=true  
APP_LOG_LEVEL=debug  
APP_URL=http://  
  
DB_CONNECTION=mysql  
DB_HOST=localhost  
DB_PORT=3306  
DB_DATABASE=meditrin_ddgi  
DB_USERNAME=meditrin_ddgi  
DB_PASSWORD=dFH=c2)/XzHD/R4  
  
GOOGLE_API_KEY=AizaSyDrxeVKav1  
  
BROADCAST_DRIVER=log  
CACHE_DRIVER=file  
SESSION_DRIVER=file  
QUEUE_DRIVER=sync  
  
REDIS_HOST=127.0.0.1  
REDIS_PASSWORD=null  
REDIS_PORT=6379  
  
MAIL_DRIVER=sendmail  
MAIL_HOST=smtp.gmail.com  
MAIL_PORT=587  
MAIL_USERNAME="ddgi.info@gmail.com"  
MAIL_PASSWORD="dFH=c  
MAIL_ENCRYPTION=tls  
  
PUSHER_APP_ID=  
PUSHER_KEY=  
PUSHER_SECRET=  
  
Admin_email=admin@
```

# Passive information gathering

- **Google Hacking**

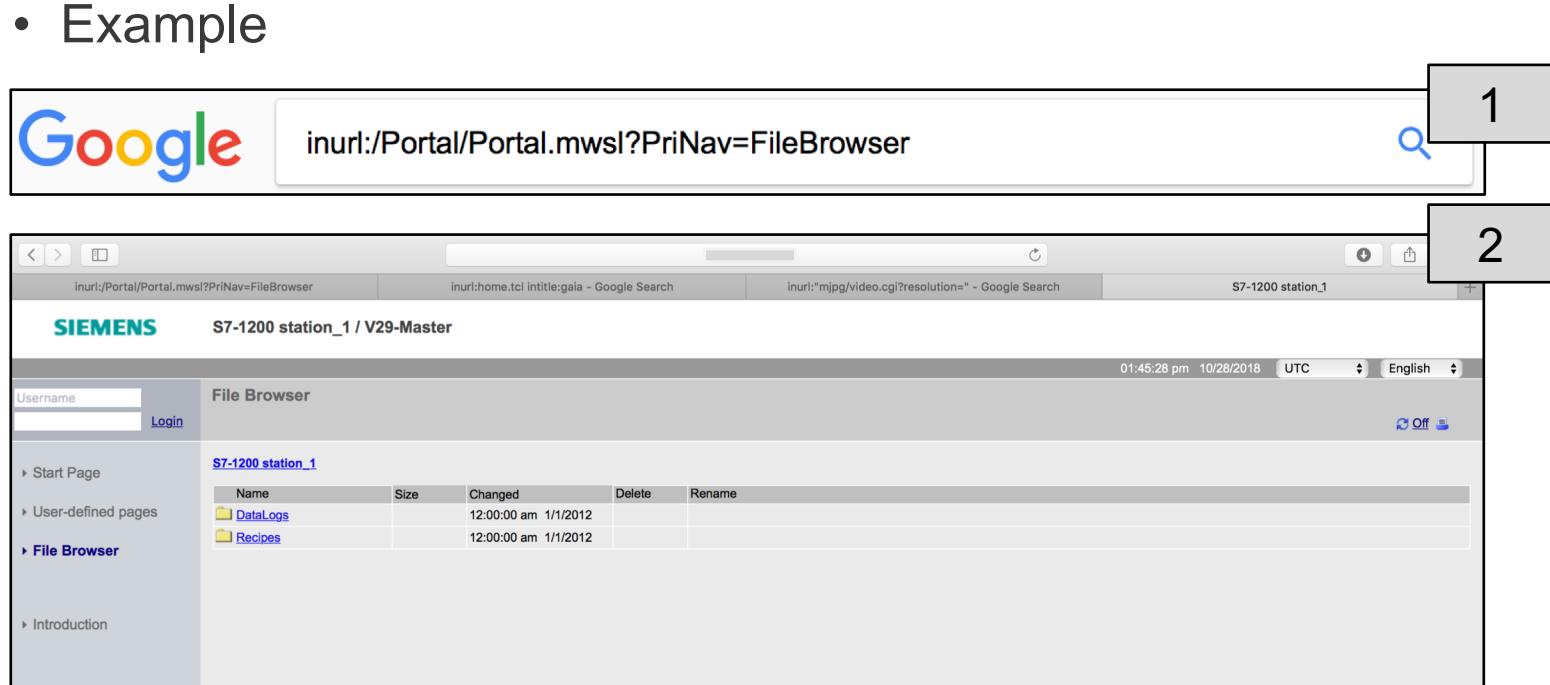
- Example



<https://www.google.com/search?q=intitle:%22SQLiteManager%22%20+%20intext:%22Welcome%20to%20SQLiteManager%20version%20%22>

# Passive information gathering

- **Google Hacking**



<https://www.google.com/search?q=inurl:/Portal/Portal.mwsl?PriNav=FileBrowser>

# Passive information gathering

- Shodan
  - The search engine for IP-hosts on the internet

The screenshot shows the Shodan search interface with the query "het:188.18.188.188" entered. The results page displays the following information:

- TOTAL RESULTS:** 185
- TOP COUNTRIES:** Denmark (185)
- TOP SERVICES:**
  - HTTPS: 87
  - HTTP: 85
  - HTTPS (8443): 4
  - 5269: 2
  - 444: 2
- TOP ORGANIZATIONS:**
  - Single allocations to customers an... (185)
- TOP OPERATING SYSTEMS:**
  - Windows Server 2008 R2 Standard... (1)

**SSL Certificate (Top Result):**

Added on 2018-11-01 11:31:47 GMT  
Denmark, Frederiksberg  
Technologies: swf,   
Details

Single allocations to customers and internal system  
SSL Certificate  
Issued By:

- Common Name: GlobalSign Organization Validation CA - SHA256 - G2
- Organization: GlobalSign nv-sa

Issued To:

- Common Name: pexipen1.
- Organization:

Supported SSL Versions: TLSv1.2

HTTP/1.1 200 OK  
Date: Thu, 01 Nov 2018 11:31:47 GMT  
Server: Apache  
X-Frame-Options: DENY  
X-XSS-Protection: 1; mode=block  
X-Content-Type-Options: nosniff  
Strict-Transport-Security: max-age=63072000; includeSubdomains;  
Last-Modified: Thu, 13 Jul 2017 13:25:51 GMT  
ETag: "1998-55432df0fb5c0"  
...

**SSL Certificate (Second Result):**

Added on 2018-11-01 10:04:24 GMT  
Denmark, Frederiksberg  
Technologies: IIS;confidence:50   
Details

innlogging  
SSL Certificate  
Issued By:

- Common Name: AlphaSSL CA - SHA256 - G2
- Organization: GlobalSign nv-sa

Issued To:

- Common Name:

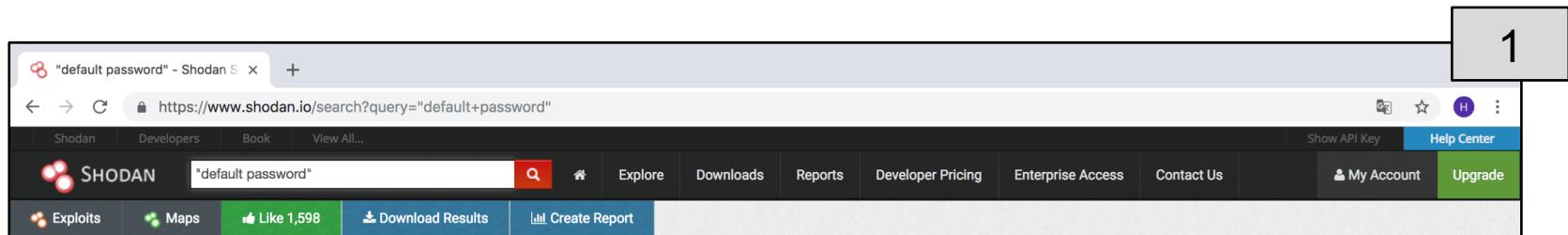
Supported SSL Versions

HTTP/1.1 200 OK  
Cache-Control: private  
Content-Type: text/html; charset=utf-8  
Server: Microsoft-IIS/7.5  
X-AspNet-Version: 4.0.30319  
X-UA-Compatible: IE=edge  
Date: Thu, 01 Nov 2018 10:04:23 GMT  
Content-Length: 9159

# Passive information gathering

- **Shodan**

- Example – Find hosts where banner information show account information.



The screenshot shows the Shodan search interface. The search bar contains the query "`default password`". The results page displays various network devices found with this specific banner string. A large grey box labeled "1" is positioned in the top right corner of the screenshot area.



The screenshot shows a 401 Unauthorized response from a Shodan search result. The response includes the following headers:

```
HTTP/1.0 401 Unauthorized
Date: Mon, 29 Oct 2018 12:16:17 GMT
Server: Boa/0.94.14rc21
Accept-Ranges: bytes
Connection: Keep-Alive
Keep-Alive: timeout=10, max=1000
WWW-Authenticate: Basic realm=" Default Name:admin Password:1234 "
Content-Type: text/html
```

A large grey box labeled "2" is positioned in the top right corner of the screenshot area.

# Passive information gathering

- **Shodan**

- Example – Find specific hosts. For example specific city, company etc.

1

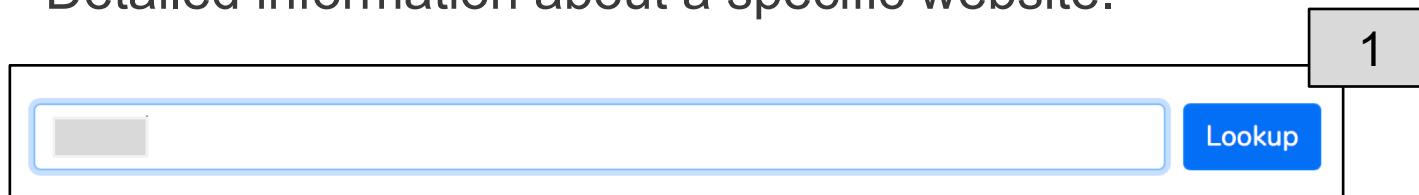
The screenshot shows the Shodan search interface. The search bar contains the query "netgear country:se city:Jönköping". Below the search bar, there are several tabs: Shodan, Developers, Book, View All..., Show API Key, Help Center, My Account, and Upgrade. At the bottom of the search bar, there are buttons for Exploits, Maps, Share Search, Download Results, and Create Report. The main area displays search results for the specified query.

2

The screenshot displays two search results from Shodan. Both results are for "HTTP 401 - Unauthorized" and are from the same host, 83.252.209.38, which is identified as "c83-252-209-38.bredband.comhem.se" and "Com Hem AB". The first result was added on 2018-10-29 09:41:57 GMT and is located in Sweden, Jönköping. The second result was added on 2018-10-29 08:11:33 GMT and is also located in Sweden, Jönköping. Both results show the same response headers: HTTP/1.1 401 Unauthorized, Content-type: text/html, WWW-Authenticate: Basic realm="NETGEAR CG3700EMR-1CMNDS", Connection: close, and Pragma: no-cache.

# Passive information gathering

- **Builtwith.com**
- Detailed information about a specific website.



Frameworks

**ASP.NET**  
ASP.NET Usage Statistics · Download List of All Websites using ASP.NET  
ASP.NET is a web application framework marketed by Microsoft that programmers can use to build dynamic web sites, web applications and XML web services. It is part of Microsoft's .NET platform and is the successor to Microsoft's Active Server Pages (ASP) technology.  
View Global Trends

**Angular**  
Angular Usage Statistics · Download List of All Websites using Angular  
Mobile and Desktop Framework.  
View Global Trends

Email Hosting Providers

**Microsoft Azure DNS**  
Microsoft Azure DNS Usage Statistics · Download List of All Websites using Microsoft Azure DNS  
This domain is verified with Microsoft Azure.  
View Global Trends

**SPF**  
SPF Usage Statistics · Download List of All Websites using SPF  
The Sender Policy Framework is an open standard specifying a technical method to prevent sender address forgery.  
Standard

# Active information gathering

- **Explore some examples.**



# Active information gathering

- **Banner grabbing**
  - Find out what version the service is running.

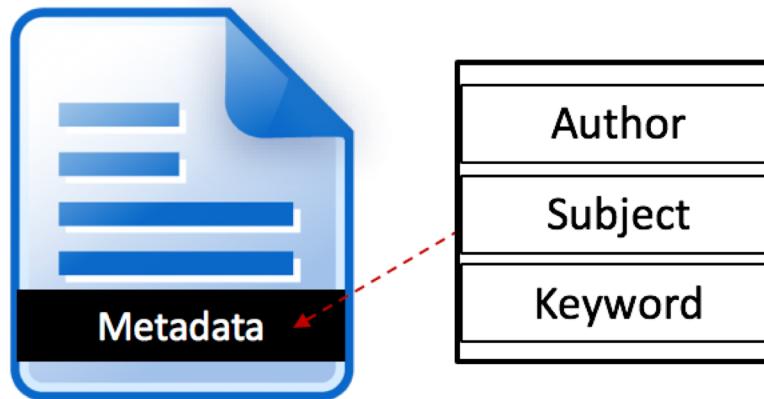
```
root@kali:~# whatweb [REDACTED]
http://[REDACTED].se [301 Moved Permanently] Country[DENMARK][DK], HTTPServer[BigIP], IP[[REDACTED]].75.240], RedirectLocation[https://www.[REDACTED].se]
https://www.[REDACTED].se/ [200 OK] Cookies[ARRAffinity], Country[DENMARK][DK], Email[info@[REDACTED]], Frame, HTML5, HttpOnly[ARRAffinity], IP[[REDACTED]]240], JQuery[2.1.1], Open-Graph-Protocol, Script[text/javascript], Strict-Transport-Security[max-age=15552000], Title[L&#246;sningar, molntj&#228;nster och produkter - Sveriges ledande it-f&#246;retag - Atea], UncommonHeaders[request-context], X-UA-Compatible[IE=edge]
```



# Active information gathering

- **Metadata in documents**

- Saves information about the author, used software, path where the documents is stored etc.
  - Often usernames is saved in the author metadata information.



# Active information gathering

- **MetadataExtractor (Python-script)**

- Extract metadata from PDF-files.

```
|\\| _ _|_ - \\\_|_ - - _|_ - -  
| |(/_|(_|/\| + |(_|(_| + ()|
```

1

```
=====
```

Håkan Sonesson, Atea

```
Usage: MetaExtractor -w <Target website> -d <Download Directory> -o <filename>
```

Example:

```
MetaExtractor -w http://www.notexist.com -d tempdir -o myfile.txt
```

```
(venv) PCSE05394:MetaExtractor hason$ python MetaExtractor.py -w http://www.notexist.com -d tempdir -o myfile.txt
```

2

```
[i] Downloading statistics.pdf...  
[+] ---> Author: percarl  
[+] ---> Creator: PScript5.dll Version 5.2.2
```

<https://gist.github.com/SecurityDragon/91f1713f0cae7a384553>

# Active information gathering

- **Brute force (Directoys and files)**
  - DirBuster (Web Application Brute Force)

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

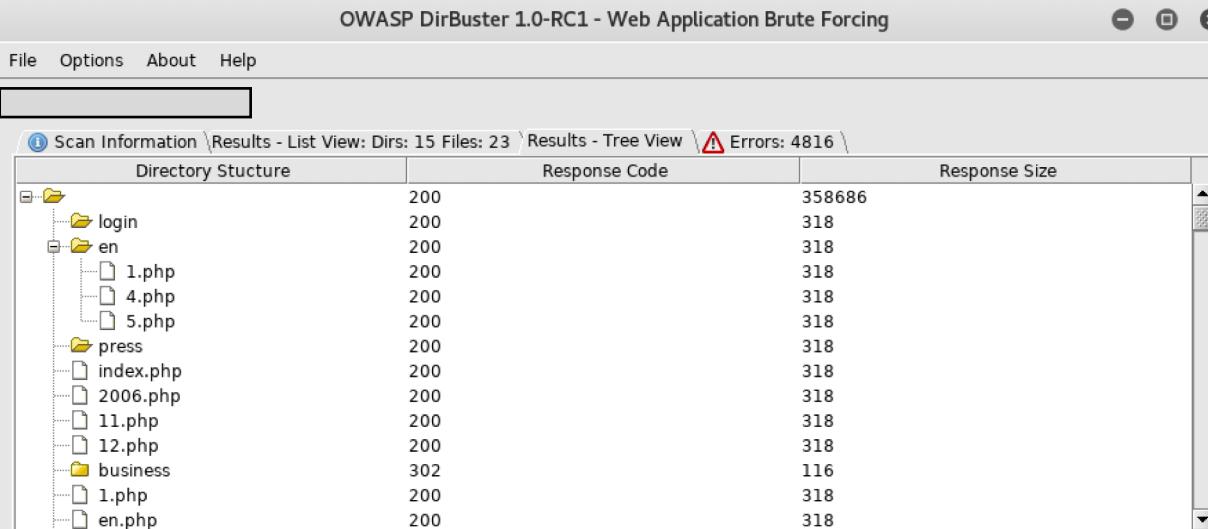
Scan Information \Results - List View: Dirs: 15 Files: 23 \Results - Tree View \ Errors: 4816 \

Directory Structure	Response Code	Response Size
...	200	358686
login	200	318
en	200	318
1.php	200	318
4.php	200	318
5.php	200	318
press	200	318
index.php	200	318
2006.php	200	318
11.php	200	318
12.php	200	318
business	302	116
1.php	200	318
en.php	200	318

Current speed: 105 requests/sec      (Select and right click for more options)  
Average speed: (T) 160, (C) 160 requests/sec  
Parse Queue Size: 0  
Total Requests: 1441/12350658  
Time To Finish: 21:26:22

Current number of running threads: 10  
[text input field] Change

Back Pause Stop Report



The screenshot shows the OWASP DirBuster application window. The title bar reads "OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing". The menu bar includes "File", "Options", "About", and "Help". Below the menu is a toolbar with several icons. The main area displays a "Scan Information" section with a tree view of scanned files and their details. The tree view shows directories like "login", "en", "press", "business", and files like "1.php", "4.php", "5.php", "index.php", etc. To the right of the tree view is a table with columns "Directory Structure", "Response Code", and "Response Size". The table lists 23 files with response codes 200 or 302 and sizes ranging from 116 to 358686. Below the table, status information is provided: Current speed (105 requests/sec), Average speed (T 160, C 160 requests/sec), Parse Queue Size (0), Total Requests (1441/12350658), and Time To Finish (21:26:22). At the bottom, there are buttons for "Back", "Pause", "Stop", and "Report". A note at the bottom right says "(Select and right click for more options)".

# Resources

- **Find out more about information gathering.**
  - Tools
    - <https://www.spiderfoot.net>
    - <https://www.elevenpaths.com/labstools/foca/index.html>
    - <https://www.paterva.com/web7/community/community.php>
    - <https://www.geocreepy.com>
    - <https://kali.org>
      - The Harvester
      - Recon-ng
      - Maltego (Community)

# Resources

- **Find out more about information gathering.**

- Websites (recourses)

- <https://censys.io>
- <https://www.shodan.io>
- <https://www.jigsawsecurityenterprise.com>
- <https://osintframework.com>
- <https://checkusernames.com>
- <https://www.exploit-db.com/google-hacking-database/>
- <https://builtwith.com>
- <https://haveibeenpwned.com>
- <https://www.beenverified.com>
- <https://www.pipl.com>
- <https://www.tineye.com>
- [https://www.owasp.org/index.php/Testing:\\_Information\\_Gathering](https://www.owasp.org/index.php/Testing:_Information_Gathering)